Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claims 1-14 (canceled).

Claim 15 (currently amended): A method for protecting a portable card, provided with a cryptographic algorithm for enciphering data and/or authenticating the card, against deriving a secret key used in the card from statistical analysis of information leaking away from the card to an outside world in the event of cryptographic operations performed by the card, the card being provided with at least a shift register having linear and non-linear feedback functions for implementing cryptographic algorithms, the method comprising the steps of:

loading data to be processed and a secret key into the shift register of the card; and

controlling the linear and non-linear feedback functions separately from each other in such a manner that collection of values of recorded leak-information signals is resistant to deriving the secret key through said statistical analysis of the values.

Claim 16 (previously presented): The method recited in claim 15 wherein said manner comprises invoking the linear and non-linear feedback functions in a predefined sequence.

Claim 17 (previously presented): The method recited in claim 15 wherein the information leaking away to the outside world comprises either power-consumption data or electromagnetic radiation.

Claim 18 (previously presented): The method recited in claim 15 further comprising the steps of:

after the key has been loaded into the shift register, clocking the shift register several times, during a specific period, using at least the linear-feedback function;

then loading data into the shift register only using the linear-feedback function; and

subsequently clocking the shift register.

Claim 19 (previously presented): The method recited in claim 18 further comprising the step of:

during a first instance of clocking the shift register, clocking the shift register for a sufficiently long time such that the contents of all elements of the shift register largely depend on bits of the key.

Claim 20 (previously presented): The method recited in claim 18 further comprising the steps of:

after the key has been loaded into the shift register, disconnecting the data from an input to the shift register; and

after the specific period has occurred, reconnecting the data to the input of the shift register so that the data can then be loaded into the shift register.

Claim 21 (previously presented): The method recited in claim 15 further comprising the step of:

after the key has been loaded into the shift register, clocking the shift register, during a specific period, several times, with the linear and non-linear feedback functions of the shift register being active but no data being loaded into the shift register during or prior to the clocking or prior to loading the key.

Claim 22 (previously presented): The method recited in claim 21 further comprising the steps of:

after the key has been loaded into the shift register, disconnecting the data from an input to the shift register; and

after the specific period has occurred, reconnecting the data to the input to the shift register so that the data can then be loaded into the shift register.

Claim 23 (previously presented): The method recited in claim 15 further comprising the step of:

loading the key into the shift register with both the linear and non-linear functions being active and only when the contents of the shift register are fixed.

Claim 24 (previously presented): The method recited in claim 15 further comprising the steps of:

if the key is not been loaded into the shift register while the contents of the shift register are fixed, loading the key into the shift register using only the linear feedback function; and

then clocking the shift register.